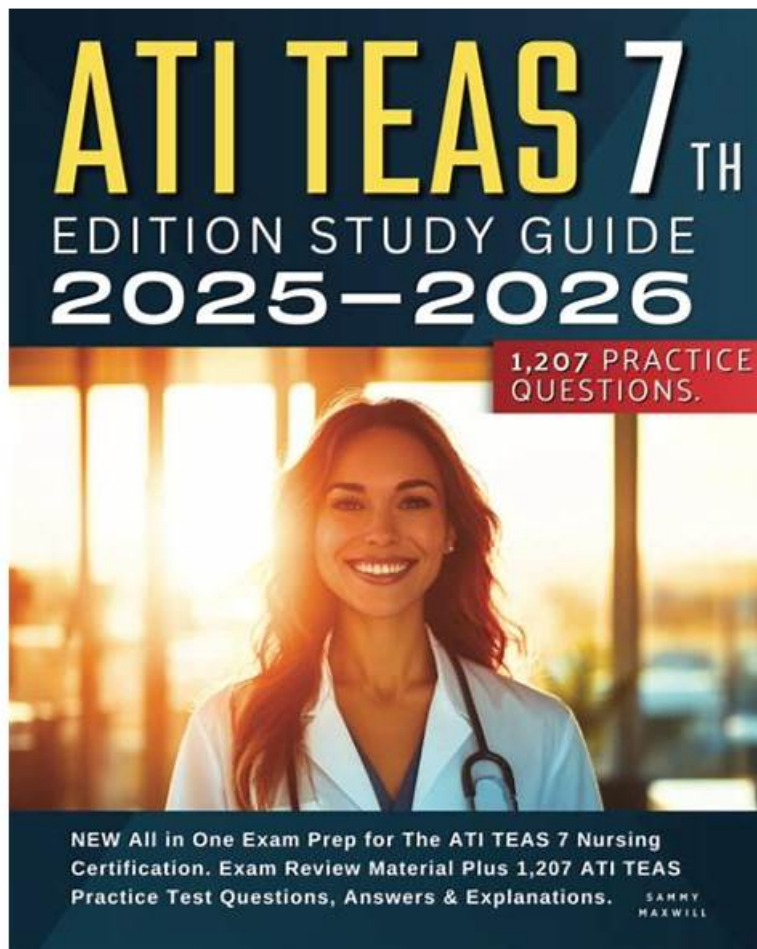


Well FCSS_ADA_AR-6.7 Prep & Reliable FCSS_ADA_AR-6.7 Test Dumps



BTW, DOWNLOAD part of Pass4guide FCSS_ADA_AR-6.7 dumps from Cloud Storage: <https://drive.google.com/open?id=1KHPWgD5jS-KShRDnmPd-8tHNpETiFHM>

Knowledge makes prominent contributions to human civilization and progress. In the 21st century, the rate of unemployment is increasing greatly. Many jobs are replaced by intelligent machines. You must learn practical knowledge such as our FCSS_ADA_AR-6.7 actual test guide, which cannot be substituted by artificial intelligence. In addition, you do not need to purchase other reference books. Our FCSS_ADA_AR-6.7 Exam Questions are able to solve all your problems of preparing the exam. Of course, our study materials are able to shorten your learning time. You will have more spare time to do other things. And we can ensure you to pass the FCSS_ADA_AR-6.7 exam.

Fortinet FCSS_ADA_AR-6.7 Exam Syllabus Topics:

Topic	Details
Topic 1	FortiSIEM Rules and Analytics: This section evaluates the expertise of Security Analysts and Automation Engineers in configuring FortiSIEM rules and analytics. It includes constructing security rules based on event patterns, leveraging MITRE ATT&CK® frameworks, and configuring advanced nested queries and lookup tables for complex threat detection and correlation.
Topic 2	FortiSIEM Baseline and UEBA: This section tests the knowledge of Compliance Officers and Threat Analysts in implementing baseline profiles and User and Entity Behavior Analytics (UEBA). It covers creating baseline reports, configuring UEBA agents, and analyzing log-based behavioral patterns to detect anomalies and insider threats.

Topic 3	• Conditions and Remediation: This section measures the skills of Incident Responders and SOAR Specialists in remediating security incidents. It includes configuring manual and automated remediation workflows, integrating FortiSOAR with FortiSIEM for streamlined incident resolution, and deploying scripts to address threats while maintaining compliance
Topic 4	• Multi-Tenancy SOC Solution for MSSP: This section of the exam measures the skills of MSSP Architects and SOC Engineers in designing and deploying multi-tenant Security Operations Center (SOC) environments using FortiSIEM. It covers defining collectors and agents, deploying FortiSIEM in hybrid setups, managing resource allocation, and installing • managing Windows and Linux agents for scalable event monitoring in multi-tenant architectures.

>> Well FCSS_ADA_AR-6.7 Prep <<

Reliable FCSS_ADA_AR-6.7 Test Dumps - FCSS_ADA_AR-6.7 Labs

You can trust the FCSS_ADA_AR-6.7 practice test and start this journey with complete peace of mind and satisfaction. The FCSS_ADA_AR-6.7 exam PDF questions will not assist you in FCSS—Advanced Analytics 6.7 Architect (FCSS_ADA_AR-6.7) exam preparation but also provide you with in-depth knowledge about the FCSS—Advanced Analytics 6.7 Architect (FCSS_ADA_AR-6.7) exam topics. This knowledge will be helpful to you in your professional life. So FCSS—Advanced Analytics 6.7 Architect (FCSS_ADA_AR-6.7) exam questions are the ideal study material for quick Fortinet FCSS_ADA_AR-6.7 exam preparation.

Fortinet FCSS—Advanced Analytics 6.7 Architect Sample Questions (Q34-Q39):

NEW QUESTION # 34

Refer to the exhibit.

Edit SubPattern

Name: ExcessVPNLoginFailure

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	IN	EventTypes: VPN Logon Failure	+	AND	+

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	COUNT(Matched Events)	>=	2	+	AND	+

Group By:

Attribute	Row	Move
Source IP	+	↑ ↓
Reporting Device	+	↑ ↓
Reporting IP	+	↑ ↓
User	+	↑ ↓

The rule evaluates multiple VPN logon failures within a ten-minute window. Consider the following VPN failure events received within a ten-minute window:

```

Reporting IP="1.1.1.1" Source
IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-
login-fail" user="Sarah"

Reporting IP="1.1.1.1" Source
IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-
login-fail" user="John"

Reporting IP="1.1.1.3" Source
IP="2.2.2.2" Reporting
Device="FortiGate2"
action="ssl-login-fail"
user="Tom"

Reporting IP="1.1.1.3" Source
IP="2.2.2.2" Reporting
Device="FortiGate2"
action="ssl-login-fail"
user="John"

Reporting IP="1.1.1.3" Source
IP="2.2.2.2" Reporting
Device="FortiGate2"
action="ssl-login-fail"
user="Sarah"

Reporting IP="1.1.1.1" Source
IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-
login-fail" user="Tom"

```

How many incidents are generated?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

Explanation:

The rule triggers an incident when there are two or more VPN logon failures within a 10-minute window, grouped by Source IP, Reporting Device, Reporting IP, and User. Let's analyze the events:

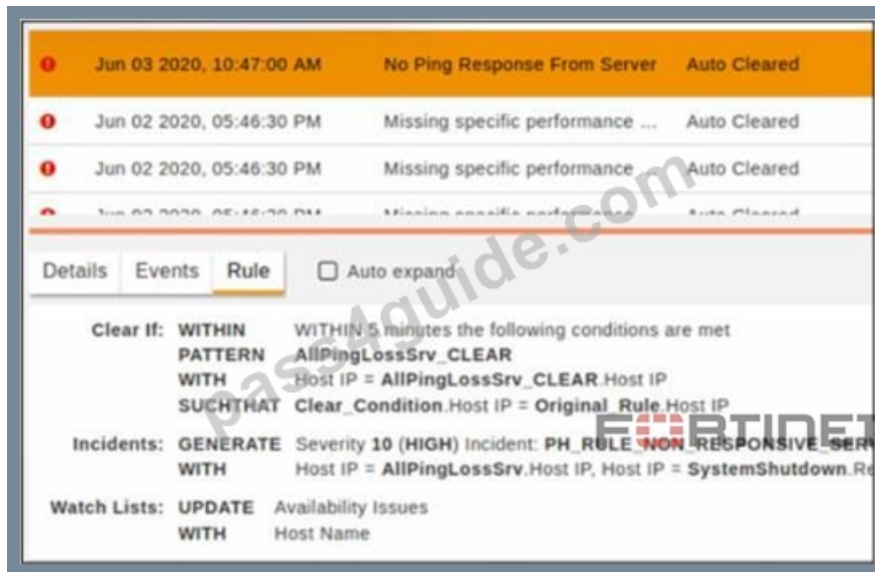
Breakdown of Events:

1. Reporting IP: 1.1.1.1, Source IP: 2.2.2.2, Device: FortiGate, User: Sarah
 2. Reporting IP: 1.1.1.1, Source IP: 2.2.2.2, Device: FortiGate, User: John
 3. Reporting IP: 1.1.1.3, Source IP: 2.2.2.2, Device: FortiGate2, User: Tom
 4. Reporting IP: 1.1.1.3, Source IP: 2.2.2.2, Device: FortiGate2, User: John
 5. Reporting IP: 1.1.1.3, Source IP: 2.2.2.2, Device: FortiGate2, User: Sarah
 6. Reporting IP: 1.1.1.1, Source IP: 2.2.2.2, Device: FortiGate, User: Tom
- Now, applying the grouping criteria (Source IP, Reporting Device, Reporting IP, and User):

- *Group 1: (1.1.1.1, 2.2.2.2, FortiGate, John) → 1 occurrence (not enough)
 - *Group 2: (1.1.1.1, 2.2.2.2, FortiGate, Sarah) → 1 occurrence (not enough)
 - *Group 3: (1.1.1.1, 2.2.2.2, FortiGate, Tom) → 2 occurrences (incident triggered)
 - *Group 4: (1.1.1.3, 2.2.2.2, FortiGate2, John) → 2 occurrences (incident triggered)
 - *Group 5: (1.1.1.3, 2.2.2.2, FortiGate2, Sarah) → 1 occurrence (not enough)
 - *Group 6: (1.1.1.3, 2.2.2.2, FortiGate2, Tom) → 1 occurrence (not enough)
- Final Incident Count:
- *One incident for Group 3 (Tom on FortiGate)
 - *One incident for Group 4 (John on FortiGate2)

NEW QUESTION # 35

Refer to the exhibit.



Why was this incident auto cleared?

- A. Within five minutes, the packet loss percentage dropped to a level where the reporting IP is same as the source IP
- B. Within five minutes, the packet loss percentage dropped to a level where the host IP of the original rule matches the host IP of the clear condition pattern
- C. Within five minutes the packet loss percentage dropped to a level where the reporting IP is the same as the host IP
- D. The original rule did not trigger within five minutes

Answer: B

NEW QUESTION # 36

Refer to the exhibit.

```
[BEGIN GLOBAL]
APP_SERVER_HOST=super.example.com
APP_SERVER_PORT=443

cust_id= 2000
agent_id=10000
reader_id=99
num_event_sequence_id=50000

[BEGIN phEventPackage]
parser_server_upload_host= worker1.example.com,worker2.example.com
svn_server_upload_host= worker1.example.com,worker2.example.com
```

What is the collector ID?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

NEW QUESTION # 37

Refer to the exhibit.

PROCESS	UPTIME
phParser	DOWN
phAgentManager	DOWN
phCheckpoint	DOWN
phDiscover	DOWN
phEventPackager	DOWN
phPerfMonitor	DOWN
phEventForwarder	DOWN
phMonitor	13:04
phMonitorAgent	DOWN
Rsyslogd	DOWN

An administrator deploys a new collector for the first time, and notices that all the processes except the phMonitor are down. How can the administrator bring the processes up?

- A. The collector was not deployed properly and must be redeployed.
- B. The administrator needs to run the command `phtools --start` all on the collector.
- C. Rebooting the collector will bring up the processes.
- D. The processes will come up after the collector is registered to the supervisor.

Answer: D

NEW QUESTION # 38

Refer to the exhibit.

edit SubPattern

Name: WMI

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	☐	Event Type	=	PH_DEV_MON_WMI_PING_STAT	☐	AND	☐

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	☐	COUNT(Matched Events)	>=	3	☐	AND	☐
	☐	AVG(Avg Round Trip Time)	>	100	☐	AND	☐
	☐	AVG(Avg Round Trip Time)	>=	1.50*STAT_AVG(AVG(Avg Round Trip Time):129)	☐	AND	☐

Group By: Attribute

Host Name

The window for this rule is 30 minutes.

What is this rule tracking?

- A. A sudden 150% increase in WMI response times over a 30-minute time window
- B. A sudden 1.50 times increase in WMI response times over a 30-minute time window
- C. A sudden 75% increase in WMI response times over a 30-minute time window
- D. A sudden 50% increase in WMI response times over a 30-minute time window

Answer: A

The rule is tracking a sudden increase in WMI response times over a 30-minute window. The key detail here is the increase factor.

*A 1.50x increase corresponds to a 150% increase, since the new value is original + 150% of original.

• • • • •

Reliable FCSS_ADA_AR-6.7 Test Dumps: https://www.pass4guide.com/FCSS_ADA_AR-6.7-exam-guide-torrent.html

- What's more, part of that Pass4guide FCSS_ADA_AR-6.7 dumps now are free: <https://drive.google.com/open?id=1KHPWgD5jS-KShrDnfmPd-8tHNpETiFHM>